This listing of claims will replace all prior versions, and listings, of claims in the present application.

LISTING OF CLAIMS:

Claim 1. (Currently Amended) A method for providing cryptographic keys usable in a network of connected computer nodes applying a signature scheme, the method executable by a first computer node comprising the steps of:

generating a random secret key;

generating an exponent interval *I* having a plurality of exponent elements, said interval having a specified first random limit, wherein, with a probability close to certainty, each element of said plurality of exponent elements of the exponent interval ~~has~~ having a unique prime factor that is larger than a given security parameter; and

providing a public key comprising an exponent-interval description including said first random limit, and an interval width specification and a public key value derived from the random secret key, said public key value including a random prime value, a number (n) corresponding to a product of two large prime numbers forming said secret key, said exponent interval, and two public values from a set of elements having a square root modulo n, such that the random secret key and a selected exponent value from the plurality of exponent elements in said exponent interval *I* are usable for deriving a signature value on a message to be sent within the network to a second computer node for verification.

Claim 2. (Original) The method according to claim 1, wherein the step of generating a random secret key comprises using two primes, the product of which is part of the public key.

Claim 3. (Original) The method according to claim 1, wherein the step of generating a random secret key comprises selecting an integer value defining a class group and selecting two elements of the class group.

Claim 4. (Original) The method according to claim 3, wherein the step of providing a public key comprises computing a modified public key value under use of the selected two elements and the exponent interval.

Claim 5. (Currently Amended) A method for providing a signature value on a message in a network of connected computer nodes, the method executable by a first computer node comprising the steps of:

selecting an exponent value from an exponent interval *I* having a plurality of exponent elements, said interval having a specified first random limit, wherein each element of said plurality of exponent elements of the exponent interval *I* has, with a probability close to certainty, a unique prime factor that is larger than a given security parameter; and

deriving the signature value from a provided secret key, the selected exponent value from said plurality of exponent elements in said exponent interval *I*, and the message, the signature value being sendable within the network to a second computer node for verification.

Claim 6. (Original) The method according to claim 5, wherein the step of deriving the signature value further comprises a computation of the i-th root of a value derived from the message and the secret key using a cryptographic hash function, the i being the exponent value.

Claim 7. (Currently Amended) A method for verifying a signature value on a message in a network of connected computer nodes, the method executable by a second computer node comprising the steps of:

receiving the signature value from a first computer node;

providing, at the second computer node, a public key comprising: an exponent-interval description having a specified first random limit and an interval width specification and, a public key value derived from the random secret key, said public key value including a random prime value, a number (n) corresponding to a product of two large prime numbers forming said secret key, an exponent interval *I* having a plurality of exponent elements, and two public values from a set of elements having a square root modulo n; and

verifying, using said provided public key value, whether an exponent value is contained in an exponent interval *I* having a plurality of exponent elements, wherein each element of said plurality of exponent elements of the exponent interval has, with a probability close to certainty, a unique prime factor that is larger than a given security parameter, the signature value [[is]] being invalid if the exponent value is not contained in the exponent interval.

Claim 8. (Original) The method according to claim 7, wherein the step of verifying further comprises a computing step of raising a computed signature root value that being part of the signature value to the power of the exponent value.

Claim 9. (Currently Amended) An apparatus to provide a signature value on a message in a network of connected computer nodes, the apparatus executable by a first computer node comprising:

means for selecting an exponent value from an exponent interval *I* having a plurality of exponent elements, wherein each element of said plurality of exponent elements of the exponent interval has, with a probability close to certainty, a unique prime factor that is larger than a given security parameter; and

means for deriving the signature value from a provided secret key, the selected exponent value, and the message, the signature value being sendable within the network to a second computer node for verification.

Claim 10. (Currently Amended) An apparatus to verify a signature value on a message in a network of connected computer nodes, the apparatus executable by a second computer node comprising:

means for receiving the signature value from a first computer node, and

means for providing, at said second computer node, a public key comprising: an exponent-interval description having a specified first random limit and an interval width specification and, a public key value derived from a random secret key, said public key value including a random prime value, a number (n) corresponding to a product of two large prime numbers forming said secret key, an exponent interval *I* having a plurality of exponent elements, and two public values from a set of elements having a square root modulo n; and

means for verifying, using said provided public key value, whether an exponent value is contained in an exponent interval *I* having said plurality of exponent elements, wherein each

element of said plurality of exponent elements of the exponent interval has, with a probability close to certainty, a unique prime factor that is larger than a given security parameter , the signature value [[is]] being invalid if the exponent value is not contained in the exponent interval *I*.

Claim 11. (Canceled)

Claim 12. (Currently Amended) An apparatus to provide cryptographic keys usable in a network of connected computer nodes applying a signature scheme, the apparatus executable by a first computer node comprising:

means for generating a random secret key;

means for generating an exponent interval *I* having a plurality of exponent elements, said interval having a first random limit, wherein, with a probability close to certainty, each element of the exponent interval has a unique prime factor that is larger than a given security parameter; and

means for providing a public key comprising: an exponent-interval description having a specified first random limit and an interval width specification, and a public key value derived from the random secret key, said public key value including a random prime value, a number (n) corresponding to a product of two large prime numbers forming said secret key, said exponent interval *I*, and two public values from a set of elements having a square root modulo n, such that the random secret key and a selected exponent value from the exponent interval *I* are usable for deriving a signature value on a message to be sent within the network to a second computer node for verification.

Claim 13 (Canceled)

Claim 14. (Currently Amended) A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for providing cryptographic keys usable in a network of connected computer nodes applying a signature scheme, said method steps comprising the steps of:

generating a random secret key;

generating an exponent interval *I* having a plurality of exponent elements, said interval having a specified first random limit, wherein, with a probability close to certainty, each element of said plurality of exponent elements of the exponent interval *I* has a unique prime factor that is larger than a given security parameter; and

providing a public key comprising: an exponent-interval description having said specified first random limit and an interval width specification, and a public key value derived from the random secret key, said public key value including a random prime value, a number (n) corresponding to a product of two large prime numbers forming said secret key, said exponent interval *I*, and two public values from a set of elements having a square root modulo n, such that the random secret key and a selected exponent value from the exponent interval are usable for deriving a signature value on a message to be sent within the network to a second computer node for verification.

Claim 15. (Canceled)

Claim 16. (Currently Amended) A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for providing a signature value on a message in a network of connected computer nodes, said method steps comprising the steps of:

selecting an exponent value from an exponent interval *I* having a plurality of exponent elements , wherein each element of said plurality of exponent elements of the exponent interval *I* has, with a probability close to certainty, a unique prime factor that is larger than a given security parameter; and

deriving the signature value from a provided secret key, the selected exponent value from said plurality of exponent elements in said exponent interval, and the message, the signature value being sendable within the network to a second computer node for verification.

Claim 17. (Canceled)

Claim 18. (Currently Amended) A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for providing a signature value on a message in a network of connected computer nodes, said method steps comprising the steps of:

receiving the signature value from a first computer node,

providing, at said second computer node, a public key comprising: an exponent-interval description having a specified first random limit and an interval width specification and, a public key value derived from a random secret key, said public key value including a random prime value, a number (n) corresponding to a product of two large prime numbers forming said secret

key, an exponent interval *I* having a plurality of exponent elements, and two public values from a set of elements having a square root modulo n; and

verifying, using said provided public key value, whether an exponent value is contained in an exponent interval *I* having a plurality of exponent elements, wherein each element of the exponent interval has, with a probability close to certainty, a unique prime factor that is larger than a given security parameter, the signature value [[is]] being invalid if the exponent value is not contained in the exponent interval.

Claim 19 – 21 (Canceled)